1007409NL USPTO 2004-1279

Translated from the D U T C H

Bureau for the Industrial Property
The Netherlands

1007409

C PATENT[6]
NL C 1007409

Date of application: October 31, 1997

IPC: H 04 L 9/32, H 04 L 9/08; H 04 Q 7/32

Date of making available to the public by viewing, or copying upon request, of an unexamined document, on which no grant has taken place on or before the said date: November 18, 1997, Industriële Eigendom 98/02

Date of making available to the public by viewing, or copying upon request, of a document, on which grant has taken place on or before the said date: November 18, 1997

Date of publication: February 8, 1998, in Industriële Eigendom 98/02
Name of grantee: Koninklijke PTT Nederland, Ltd. in Groningen, NL

Inventor: Sharon Christie Lesley Prins, [residing] in Groningen,
Patent agents: Engineer G. J. Baas, residing in 2509 CH, The Hague.

[Title in Dutch of the object of the invention:]
Authenticatiesyteem

AUTHENTICATION SYSTEM

(54) Authentication system, whereby a user or subscriber of a system can verify his/her identity with respect to this system (3) as a result of the input of an authentication code by this system, which code is examined by the system to establish validity. The authentication code [identification code] is generated by a generator (4), and, on the one hand, it is transmitted onto the system, which requests authentication [identification]. On the other hand, the code is transmitted to the user or subscriber on account of the addressing to a unique address, provided by the user. As a matter of course, the transmission medium, should be "intruder-proof". Preferably, use is made of a strictly personal user terminal, as well os of a GSM-terminal, which is provided with a " Security & Identification Module" (SIM).

*

* *

* *

Authentication System

BACKGROUND OF THE INVENTION

The invention pertains to an authentication system [system for the verification of the identity of an user] whereby a user or subscriber of a system verifies his or her identity with

respect to that system as a result of the input with the help of that system of an authentication [identification] code, which is examined by the system for validity.

Generally speaking, such an authentication system is known. Alphanumeric "passwords" are often used for the purpose of authentication, which "passwords" are input by the user, using a keyboard. If a fixed or permanent password is used, the disadvantage of such a use is that the password can be stolen or copied, and, after that, misused. For that reason, there also exist "one-time password" (OTP) systems, whereby a password is used only once.

SUMMARY OF THE INVENTION

The invention provides for an OTP system whereby the OTP, which is generated by an OTP generator, is - one the one hand - transmitted to the system, which asks for authentication, and that OTP - on the other hand - is transmitted to the user whereby the OTP is addressed to a unique user address. As a matter of course,, the transmission medium should be "intruder-proof". Preferably, use is made of a strictly personal user-terminal, as well as of a (GSM) terminal, which is provided with a "Security & Identification Module" (SIM).

The invention will be elucidated in greater detail as follows by means of an exemplified embodiment.

EXEMPLIFIED EMBODIMENT

Fig. 1 illustrates in a rather diagrammatic way an exemplified embodiment of the invention. To a network 1 (Internet), which is suitable for IP* [*Translator's note: The inventor has not specifically mentioned what IP stands for. IP stands for information provider. But it also stands for information processing; and for internetwork protocol).], there is connected a terminal 2, a server 3, and an authentication [identification server] 4. To a network 6, suitable for GSM, there are connected a "Short Message Service" (SMS) server 5 and a base station 7, which is capable of establishing a connection with a GSM terminal 8. As a matter of course, there are much more terminals, servers, etc. in reality.

The mode of operation of the authentication system in accordance with the invention, embodied in the system, depicted in Fig. 1, is as follows.

By way of terminal 2, and the Internet 1, a user or subscriber establishes a connection with server 3, in order to make use of a service, for which purpose an authentication or verification of the identity of the user, is necessary. To this end, the server 3 sends an HTML-coded message to the terminal, wherein the user is requested to input the number of his/her mobile phone 8. The server 3 transmits a request to the authentication server 4 to generate a (random) authentication

[identification] code, and to have the code sent to the user. After this, the server 3 transmits to the user the request to wait for an SMS-message, having the requested authentication code, which the user is to receive on his/her mobile telephone set. Meanwhile, the code is generated by server 4, and is transmitted to SMS-server 5 as well as to server 3. The SMS-server forwards the code, in the form of a SMS-message, to the mobile telephone set 8, which displays the received code on the display or miniature viewing screen. The suer reads this, and relays the code by way of his/her terminal to the server 3. The latter compares the code, received by the terminal 2 with the code, which is (directly) received by the server 4. In the case of a conformity, the service, requested by the user, is cleared or allowed.

It ought to be noticed that the links between the servers 3, 4 and 5 should indeed be secure. There can be just materialized (differently from what the figure depicts) connections just outside the IP or, indeed, via the IP, but then secured, e.g., by means of "firewalls", etc. Server 4 can also be incorporated in server 3, as a result of which the security is also improved.

Instead of a single telephone set, other kinds of receivers can also be used, e.g., a paging receiver. However, that kind of receiver is nowadays less "intruder-proof" than the today's GSM-terminals. Also, it is not intrinsically necessary to make use of a radio-receiver. Each medium is suitable, provided that the

"link" of the code-generator (authentication server) to the receiver, in the immediate proximity of the user, is sufficiently secure. In principle, the same medium, with which the terminal has connection with the server (3) which asks about authentication, can be used as medium. For example, a secured virtual channel of a "Virtual Private Network" (VPN) can be sued as medium.

Above, it was proposed that the user reads the received authentication code (off the display of his/her GSM* set), and the server 3 relays the code by way of his/her keyboard to be overwritten. ('Translator's note : GSM = Global System for Mobile Communication.) As soon as presented, it is of course nicer to directly forward the code, received at the user's location, to the server 3 without a need to overwrite it. For example, this can be done by means of local, direct data connection between the GSM-receiver and the data terminal 2. The data terminal can - by way of an application program, suitable for that purpose - read in [input] the received authentication code, and relay it to the server 3. Also, the authentication-code receiver 8 can be integrated into the terminal 2. If the same medium could be used for the connection between the terminal 2 and the server 3, in this case the Internet 1, such a direct relay of the locally received authentication code is even more obvious. The process comprises then the following steps:

- server 3 queries terminal 2 for authentication code;

- server 3 requests server 4 to generate an authentication code;

- server 4 generates an authentication code, and transmits it to server 3, and to a user terminal: thus, in the preceding, via a GSM-SMS (server 5, network 6 and radiolink 7 - 8), or, as an alternative, via a "secure" [sic] connection via the IP network 1 to the terminal 2;

- the local user retrieves [copies] the received authentication code, and transmits it to server 3; in the case of a direct local link, the authentication code is locally received, via GSM or via IP, and, after that, transmitted by means of the terminal 2 to server 3; in that latter case, the user does not need to do anything; the authentication process for the users can take place even "under water".

CLAIMS

1. Authentication system, in accordance with which a local user or subscriber can verify his/her identity with respect to a system as a result of the input - with the help of that system by way of a local terminal (2) - of an authentication [identification] code, which is examined by that system for validity, c h a r a c t e r i z e d i n t h a t the authentication code is generated by a code-generator (4), which - on the one hand - transmits the generated code onto the system

(3), which ask for authentication, and - on the other hand - addresses and transmits the generated code to a local code-receiver (8), having an own receive identifier [address] whereupon the user transmits the authentication code thus received to the system (3)asking for it.

2. Authentication system, as claimed in claim 1, c h a r a c t e r i z e d i n t h a t the local code-receiver has a local connection or link with the said local terminal (2).

3. Authentication system, as claimed in claim 1, c h a r a c t e r i z e d i n t h a t the local code-receiver constitutes part of the local terminal (2).

4. Authentication system, as claimed in claim 1, c h a r a c t e r i z e d i n t h a t different media (1, 6) are used for the connection between the local terminal (2) and the server (3), on the one hand, and the connection between the code-generator (4) and the local code-receiver (8), on the other hand.

5. Authentication system, as claimed in claim 1, c h a r a c t e r i z e d i n t h a t the same, common medium, although different channels within that same medium, is used for the connection between the local terminal (2) and the server (3), on the one hand, and the connection between the code-generator (4) and the local code-receiver (8), on the other hand.

6. Authentication system, as claimed in claim 4,

c h a r a c t e r i z e d i n t h a t the local code-receiver is formed by a mobile voice- or date-terminal.

7. Authentication system, as claimed in claim 6, c h a r a c t e r i z e d i n t h a t the local code-receiver is formed by a digital mobile terminal as well as by a GSM-terminal.

8. Authentication system, as claimed in claim 4, c h a r a c t e r i z e d i n t h a t the local code-receiver is formed by a paging terminal.

USDOC/USPTO/STIC/Translations Branch
Translated by drs. John M Koytcheff, M.Sc. (Civil Engrg. & Water Engrg); WHO Fellow (Environmental Engrg.); USNWC Grad.
USPTO Translator (from GERMAN and the principal GERMANIC languages, including DUTCH)
December 31, 2003

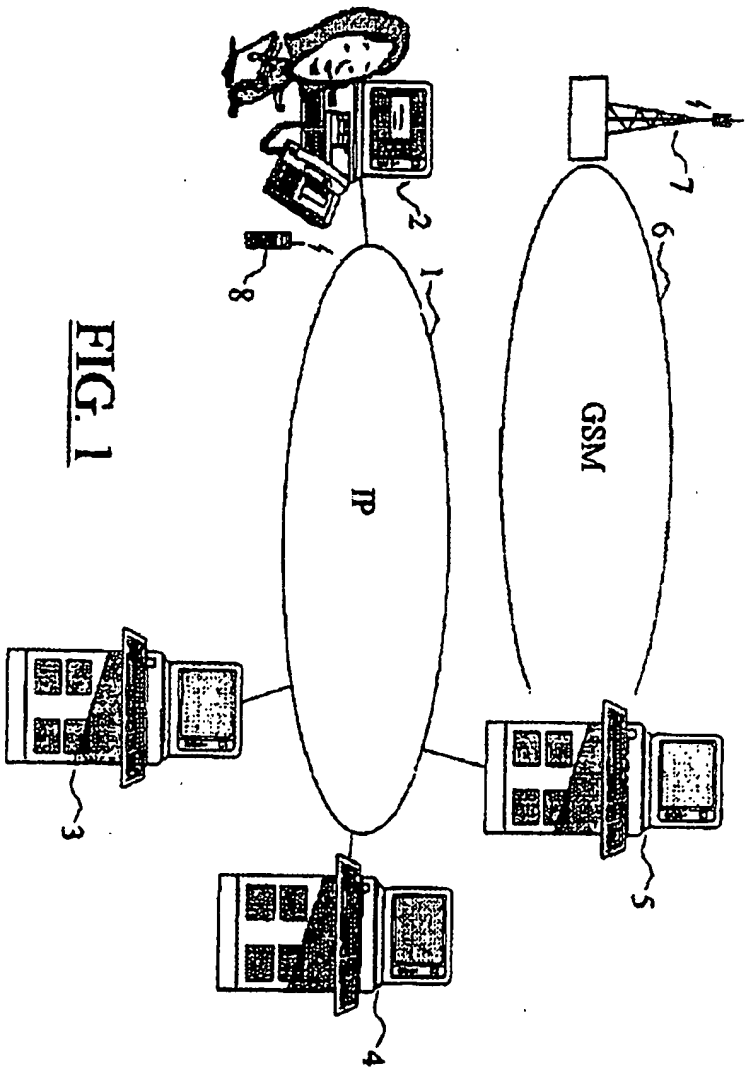


FIG. 1

(19) Bureau voor de Industriële Eigendom Nederland

(11) 1007409

(12) C OoctrooI[6]

(21) Aanvrage om octrooi: 1007409

(22) Ingediend: 31.10.97

(51) Int.Cl.[6]
H04L9/32, H04L9/08, H04Q7/32

(41) Ingeschreven:
18.11.97 I.E. 98/02

(47) Dagtekening:
18.11.97

(45) Uitgegeven:
02.02.98 I.E. 98/02

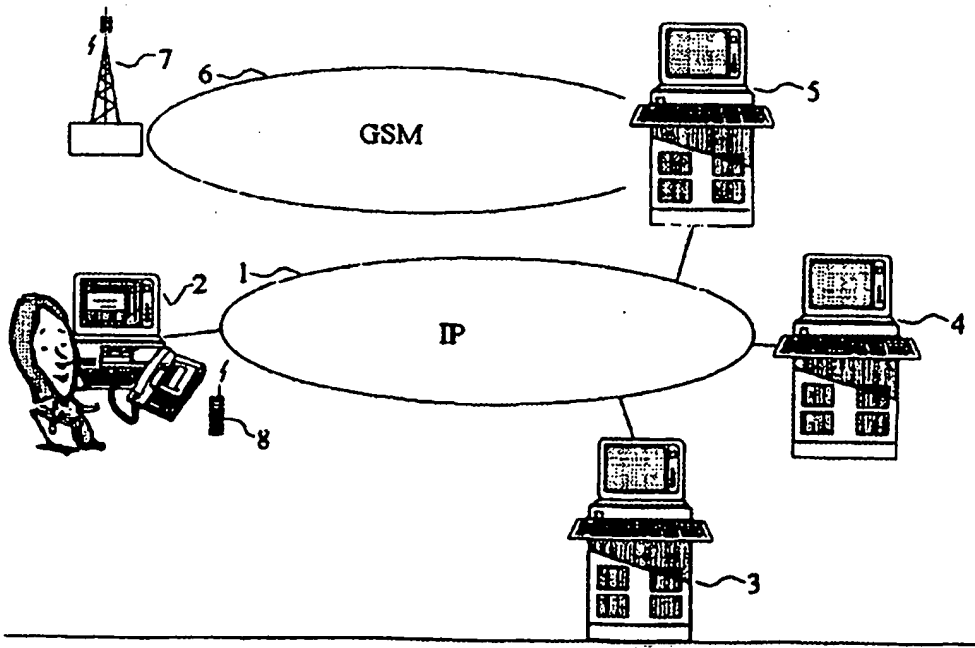
(73) Octrooihouder(s):
Koninklijke PTT Nederland N.V. te Groningen.

(72) Uitvinder(s):
Sharon Christie Lesley Prins te Groningen

(74) Gemachtigde:
Ir. G.J. Baas te 2509 CH Den Haag.

(54) **Authenticatiesysteem.**

(57) Authenticatiesysteem, waarbij een gebruiker van een systeem zich authenticeert tegenover dat systeem (3) door middel van het bij dat systeem invoeren van een authenticatiecode, welke door het systeem op geldigheid wordt onderzocht. De authenticatiecode wordt door een generator (4) gegenereerd en wordt enerzijds aan het systeem overgedragen dat om authenticatie vraagt. Anderzijds wordt de code aan de gebruiker overgedragen, door het te adresseren aan een uniek, door de gebruiker opgegeven adres. Uiteraard dient het overdrachtsmedium "intruder proof" te zijn. Bij voorkeur wordt gebruik gemaakt van een strikt persoonlijke gebruikersterminal, zoals een (GSM) terminal die is voorzien van een "Security & Identification Module" (SIM).



NL C 1007409

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekeningen.

PTO 2004-1279
S.T.I.C. Translations Branch

Authenticatiesysteem

ACHTERGROND VAN DE UITVINDING

De uitvinding heeft betrekking op een authenticatiesysteem, waarbij een gebruiker van een systeem zich authenticeert tegenover dat systeem door middel van het bij dat systeem invoeren van een authenticatiecode, welke door het systeem op geldigheid wordt onderzocht.

Een dergelijk authenticatiesysteem is van algemene bekendheid. Vaak worden voor authenticatie alfanumerieke "passwords" gebruikt, die door de gebruiker worden ingetoetst. Als een vast password wordt gebruikt, heeft dat het bezwaar dat het password ontvreemd of gecopieerd en daarna misbruikt kan worden. Om die reden bestaan er ook "one time password" (OTP) systemen, waarbij een password slechts één keer wordt gebruikt.

SAMENVATTING VAN DE UITVINDING

De uitvinding voorziet in een OTP systeem waarbij het OTP, dat door een OTP generator gegenereerd wordt, enerzijds aan het systeem wordt overgedragen dat om athenticatie vraagt, en dat anderzijds aan de gebruiker wordt overgedragen, waarbij het OTP wordt geadresseerd aan een uniek gebruikersadres. Uiteraard dient het overdrachtsmedium "intruder proof" te zijn. Bij voorkeur wordt gebruik gemaakt van een strikt persoonlijke gebruikersterminal, zoals een (GSM) terminal die is voorzien van een "Security & Identification Module" (SIM).

De uitvinding zal hierna aan de hand van een uitvoeringsvoorbeeld nader worden uiteengezet.

UITVOERINGSVOORBEELD

Figuur 1 toont zeer schematisch een uitvoeringsvoorbeeld van de uitvinding. Op een voor IP geschikt netwerk 1 (internet) is een terminal 2 aangesloten, een server 3 en een authenticatieserver 4. Op een voor GSM geschikt netwerk 6 is een "Short Message Service" (SMS) server 5 aangesloten en een basisstation 7, die verbinding kan maken met een GSM terminal 8. Uiteraard zijn er in werkelijkheid veel meer terminals, servers etc.

De werking van het authenticatiesysteem volgens de uitvinding, uitgevoerd in het in figuur 1 getoonde stelsel is als volgt.

Een gebruiker maakt via terminal 2 en het internet 1 verbinding met server 3 om daar van een service gebruik te maken waarvoor authenticatie nodig is. De server 3 stuurt daartoe een HTML gecodeerd bericht naar de terminal, waarin de gebruiker verzocht wordt het telefoonnummer van haar mobiele telefoon 8 in te voeren. De server 3 verstuurt een verzoek naar authenticatieserver 4 om een (random) authenticatiecode te genereren en naar de gebruiker te doen uitzenden. Daarna zendt de server 3 aan de gebruiker het verzoek om te wachten op een op haar mobiele telefoontoestel te ontvangen SMS-bericht met de gevraagde authenticatiecode. Intussen wordt die code door server 4 gegenereerd en naar zowel SMS server 5 als naar server 3 verstuurd. De SMS server 5 verzendt de code, in de vorm van een SMS-bericht, naar het mobiele telefoontoestel 8, dat de ontvangen code op het beeldschermpje toont. De gebruiker leest dat en geeft de code via haar terminal aan de server 3 door. Deze vergelijkt de van de terminal 2 ontvangen code met de (direct) van de server 4 ontvangen code. Bij overeenstemming wordt de door de gebruiker gevraagde service vrijgegeven.

Opgemerkt wordt dat de links tussen de servers 3, 4 en 5 wel veilig dienen te zijn. Het kunnen (anders dan de figuur aangeeft) verbindingen buiten het IP net zijn of wel via het IP net gerealiseerd zijn, maar dan beveiligd, bijvoorbeeld door "firewalls" etc. Server 4 kan ook geïncorporeerd zijn in server 3, hetgeen de veiligheid eveneens verhoogt.

In plaats van een telefoontoestel, kan ook gebruik gemaakt worden van andere soorten ontvangers, bijvoorbeeld een paging-ontvanger. Dit soort ontvangers is heden ten dage echter minder "intruder-proof" dan de huidige GSM-terminals. Ook is het niet persé nodig om van een radio-ontvanger gebruik te maken: elk medium is geschikt, mits de "link" van de codegenerator (authenticatieserver) naar de ontvanger bij de gebruiker voldoende veilig is. In principe kan als medium hetzelfde medium worden gebruikt als waarmee de terminal verbinding heeft met de server (3) die om authenticatie vraagt. Als medium kan bijvoorbeeld een beveiligd virtueel kanaal of een "Virtual Private Network" (VPN) worden gebruikt.

In het bovenstaande wordt voorgesteld dat de gebruiker de ontvangen authenticatiecode afleest (van het scherm van haar GSM toestel) en aan de server 3 doorgeeft door die code via haar toetsenbord over te

typen. Op zich is het natuurlijk fraaier om de op de gebruikerlocatie ontvangen authenticatiecode direct naar de server 3 te verzenden zonder die te hoeven overtypen. Bijvoorbeeld zou dat kunnen door een lokale, directe dataverbinding te gebruiken tussen de GSM-ontvanger en de dataterminal 2. De dataterminal kan --via een daartoe geëigend applicatieprogramma-- de ontvangen authenticatiecode inlezen en aan server 3 doorgeven. Ook kan de authenticatiecode-ontvanger 8 in de terminal 2 geïncorporeerd worden. Wanneer hetzelfde medium zou worden gebruikt als voor de verbinding tussen de terminal 2 en de server 3, in casu het internet 1, ligt een dergelijke directe doorgifte van de lokaal ontvangen authenticatiecode nog meer voor de hand. Het proces is dan:

- server 3 vraagt terminal 2 om authenticatiecode;
- server 3 verzoekt server 4 om een authenticatiecode te genereren;
- server 4 genereert een authenticatiecode en zendt die naar server 3 en naar een gebruikersterminal: in het voorgaande dus via GSM-SMS (server 5, netwerk 6 en radioverbinding 7-8), of, als alternatief, via een "secure" verbinding via het IP netwerk 1, naar de terminal 2;
- de lokale gebruiker neemt de ontvangen authenticatiecode over en zendt die naar server 3; bij een directe lokale koppeling wordt de authenticatiecode lokaal ontvangen, via GSM of via IP, en nadien door de terminal 2 naar server 3 gezonden; in dat laatste geval hoeft de gebruiker dus niets te doen; zelfs kan het authenticatieproces voor de gebruikere "onder water" plaatshebben.

CONCLUSIES

1. Authenticatiesysteem, waarbij een lokale gebruiker zich tegenover een systeem authenticeert door het, via een lokale terminal (2), bij dat systeem invoeren van een authenticatiecode, die door dat systeem op geldigheid wordt onderzocht, m e t h e t k e n m e r k d a t de authenticatiecode gegenereerd wordt door een codegenerator (4), die de gegenereerde code enerzijds overgedraagt aan het systeem (3) dat om athenticatie vraagt, en anderzijds adresseert en overdraagt aan een lokale code-ontvanger (8) met een eigen ontvangstadres, waarna de gebruiker de aldus ontvangen authenticatiecode aan het daarom vragende systeem (3) overdraagt.

2. Authenticatiesysteem volgens conclusie 1, m e t h e t k e n m e r k d a t de lokale code-ontvanger een lokale verbinding heeft met de genoemde lokale terminal (2).

3. Authenticatiesysteem volgens conclusie 1, m e t h e t k e n m e r k d a t de lokale code-ontvanger deel uitmaakt van de lokale terminal (2).

4. Authenticatiesysteem volgens conclusie 1, m e t h e t k e n m e r k d a t voor de verbinding tussen de lokale terminal (2) en de server (3) enerzijds, en de verbinding tussen de codegenerator (4) en de lokale code-ontvanger (8) anderzijds, gebruik wordt gemaakt van verschillende media (1, 6).

5. Authenticatiesysteem volgens conclusie 1, m e t h e t k e n m e r k d a t voor de verbinding tussen de lokale terminal (2) en de server (3) enerzijds, en de verbinding tussen de codegenerator (4) en de lokale code-ontvanger (8) anderzijds, gebruik wordt gemaakt van hetzelfde, gemeenschappelijke medium, zij het van verschillende kanalen binnen datzelfde medium.

6. Authenticatiesysteem volgens conclusie 4, m e t h e t k e n m e r k d a t de lokale code-ontvanger gevormd wordt door een mobiele spraak- of dataterminal.

7. Authenticatiesysteem volgens conclusie 6, m e t h e t k e n m e r k d a t de lokale code-ontvanger wordt gevormd door een digitale mobiele terminal, zoals een GSM-terminal.

8. Authenticatiesysteem volgens conclusie 4, m e t h e t k e n m e r k d a t de lokale code-ontvanger wordt gevormd door een paging-terminal.

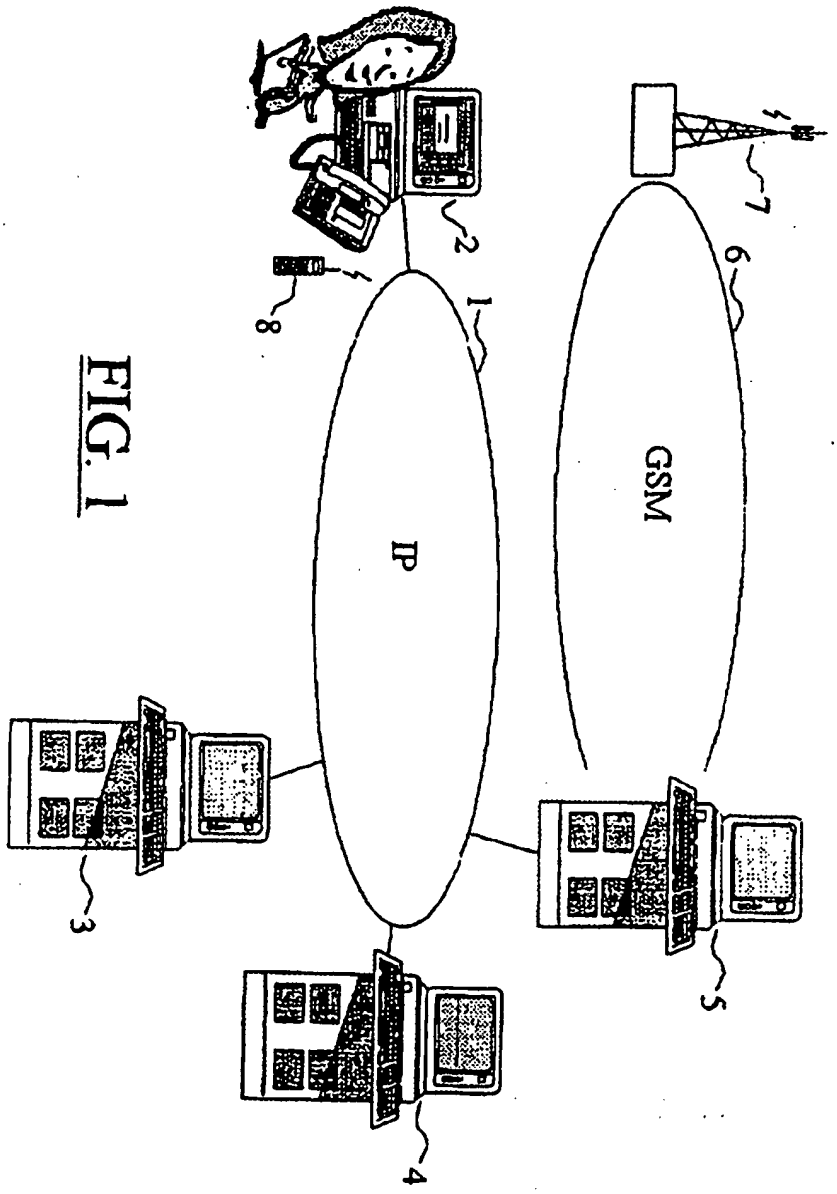


FIG. 1